Attorney Docket No. 1293.1956

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Hyun-kwon CHUNG

Application No.: Unassigned

Group Art Unit: Unassigned

Filed: September 30, 2003

Examiner: Uassigned

For: NETWORK ACCESSIBLE APPARATUS, SECURITY METHOD USED BY THE APPARATUS, AND INFORMATION STORAGE MEDIUM THAT IS REPRODUCIBLE BY THE APPARATUS

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Korean Patent Application No(s). 2002-59400

Filed: September 30, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: September 30, 2003

By: _____

Michael D. Stein
Registration No. 37,240

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

KOREAN INDUSTRIAL PROPERTY OFFICE

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

Application Number: Patent Application No. 2002-59400

Date of Application: 30 September 2002

Applicant(s): Samsung Electronics Co., Ltd.

27 November 2002

COMMISSIONER

1020020059400 2002/11/28

[Document Name]	Patent Application
[Application Type]	Patent
[Receiver]	Commissioner
[Reference No]	0007
[Filing Date]	2002.09.30.
[IPC No.]	G06F

[Title] Network accessable apparatus, security method therefor and information storage medium thereof

[Applicant]
Name: Samsung Electronics Co., Ltd.
Applicant code: 1-1998-104271-3

[Attorney]
Name: Young-pil Lee
Attorney's code: 9-1998-000334-6
General Power of Attorney Registration No. 1999-009556-9

[Attorney]
Name: Hae-young Lee
Attorney's code: 9-1999-000227-4
General Power of Attorney Registration No. 2000-002816-9

[Inventor]
Name: Hyun-kwon Chung
I.D. No. 721217-1042731
Zip Code 464-800
Address: 104-906 Dongbo Apt., Tanbeol-ri, Gwangju-eup, Gwangju-gun, Gyeonggi-do
Nationality: KR

[Application Order] We file as above according to Art.42 of the Patent Law.
Attorney Young-pil Lee
Attorney Hae-young Lee

[Fee]

Basic page:	20 Sheet(s)	29,000 won
Additional page:	16 Sheet(s)	16,000 won
Priority claiming fee:	0 Case(s)	0 won
Examination fee:	0 Claim(s)	0 won
Total:		45,000 won

[Enclosures]
1. Abstract and Specification (and Drawings) 1 copy each

대한민국 특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0059400
Application Number PATENT-2002-0059400

출 원 년 월 일 : 2002년 09월 30일
Date of Application SEP 30, 2002

출 원 인 : 삼성전자 주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2002 년 11 월 27 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0007
【제출일자】	2002.09.30
【국제특허분류】	G06F
【발명의 명칭】	네트워크에 접근가능한 장치, 그 보안 방법 및 정보저장매체
【발명의 영문명칭】	Network accessable apparatus, security method therefor and information storage medium thereof
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	1999-009556-9
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2000-002816-9
【발명자】	
【성명의 국문표기】	정현권
【성명의 영문표기】	CHUNG,Hyun Kwon
【주민등록번호】	721217-1042731
【우편번호】	464-800
【주소】	경기도 광주군 광주읍 탄벌리 동보아파트 104동 906호
【국적】	KR
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이영필 (인) 대리인 이해영 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	16	면	16,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원
【합계】	45,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

네트워크에 접근가능한 장치, 그 보안 방법 및 정보저장매체가 개시된다.

본 발명에 따른 네트워크에 접근가능한 장치에 적용가능한 보안 방법은 (a) 소정 컨텐트를 읽어오라는 명령을 내린 컨텍스트가 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 판별하는 단계; (b) 비신뢰 컨텍스트이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 단계; (c) 상기 컨텍스트가 신뢰 컨텍스트이면 상기 명령이 신뢰 요구인지 비신뢰 요구인지 여부를 판별하는 단계; (d) 상기 명령이 신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 신뢰 컨텍스트를 생성하는 단계; 및 (e) 상기 명령이 비신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 단계를 포함하는 것을 특징으로 한다. 이에 의해, 네트워크로부터 읽어들인 컨텐트에 대응하는 컨텍스트가 장치에 저장된 중요한 정보를 파괴시키거나 외부로 유출하는 등의 경우를 방지할 수 있다.

【대표도】

도 1

【명세서】

【발명의 명칭】

네트워크에 접근가능한 장치, 그 보안 방법 및 정보저장매체{Network accessable apparatus, security method therefor and information storage medium thereof}

【도면의 간단한 설명】

도 1은 본 발명에 따른 보안 방법이 구현되는 보안 시스템의 개요도,

도 2는 재생 장치(1)에 의해 컨텍스트가 로드된 메모리의 구조도,

도 3은 도 1의 재생 장치(1)의 일 실시예,

도 4는 도 3의 디스크(100)에 컨텐트의 예로서 기록된 마크업 문서 및 자바 프로그램이 해석되고 실행됨으로써 생성되는 컨텍스트를 설명하기 위한 참고도,

도 5는 도 1의 재생 장치(1)의 다른 실시예,

도 6은 도 5의 디스크(300)에 컨텐트의 일 예로서 마크업 문서가 해석되고 실행됨으로써 각각 생성되는 컨텍스트를 설명하기 위한 참고도,

도 7은 도 5의 디스크(300)에 컨텐트의 다른 예로서 마크업 문서 및 자바 프로그램이 해석되고 실행됨으로써 각각 생성되는 컨텍스트를 설명하기 위한 참고도

도 8은 본 발명의 일 실시예에 따른 보안 방법을 설명하기 위한 플로우챠트,

도 9는 본 발명의 다른 실시예에 따른 보안 방법을 설명하기 위한 플로우챠트이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<10> 본 발명은 네트워크에 접근가능한 장치에 적용가능한 보안 모델에 관한 것으로, 보다 상세하게는 네트워크에 접근가능한 장치, 그 보안 방법, 및 정보저장매체에 관한 것이다.

<11> 네트워크에 접근가능한 장치는 네트워크에 존재하는 다양한 컨텐트를 읽어올 수 있다. 예를 들면, 사용자는 웹브라우저가 탑재되어 있는 컴퓨터를 사용하여 인터넷에 존재하는 컨텐트를 가져올 수 있다. 컨텐트는 다양한 데이터, 가령 텍스트 파일, 이미지 파일, 동영상 파일, 자바 프로그램, 스크립트 프로그램, 마크업 문서 등 프리젠테이션가능한 파일(presentationable file)을 의미하며, 네트워크에 존재할 수 있음은 물론 하드디스크 등 로컬 저장 장치에도 존재할 수 있다. 컨텐트 중 마크업 문서나 자바 프로그램과 같은 어플리케이션은 해석되고 실행되어 컨텍스트로 생성된다. 컨텍스트는 컨텐트가 해석되고 실행되어 프리젠테이션된 인스턴스(instance)를 가리킨다.

<12> 그러나, 컨텍스트가 네트워크로부터 가져온 컨텐트로부터 생성된 것일 경우 그 관리에 유의해야 한다. 왜냐하면, 네트워크로부터 로컬 장치로 가져온 컨텐트로부터 생성된 컨텍스트가 로컬 장치에 저장된 중요한 사용자 정보를 알아낸 다음 몰래 네트워크의 서버로 보내거나 로컬 장치에 보관해둔 중요한 정보를 파괴시킬 수도 있기 때문이다. 즉, 네트워크에 존재하는 컨텐트는 신뢰성을 담보하기 어려우므로 이에 대한 대책이 요구된다.

【발명이 이루고자 하는 기술적 과제】

<13> 따라서, 본 발명의 목적은 네트워크에 접근가능한 장치에 있어서 네트워크로부터 읽어들인 컨텐트에 대한 보안을 강화할 수 있는 보안 방법, 그 장치 및 정보저장매체를 제공하는 것이다.

【발명의 구성 및 작용】

<14> 상기 목적은 본 발명에 따라, 네트워크에 접근가능한 장치에 적용가능한 보안 방법에 있어서, (a) 소정 컨텐트를 읽어오라는 명령을 내린 컨텍스트가 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 판별하는 단계; (b) 비신뢰 컨텍스트이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 단계; (c) 상기 컨텍스트가 신뢰 컨텍스트이면 상기 명령이 신뢰 요구인지 비신뢰 요구인지 여부를 판별하는 단계; (d) 상기 명령이 신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 신뢰 컨텍스트를 생성하는 단계; 및 (e) 상기 명령이 비신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 단계를 포함하는 것을 특징으로 하는 방법에 의해 달성된다.

<15> 또한, 상기 목적은 네트워크에 접근가능한 장치에 적용가능한 보안 방법에 있어서, (a) 컨텍스트가 동작 명령을 내리는 단계; (b) 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 판별하는 단계; (c) 비신뢰 컨텍스트이면 상기 동작 명령의 실행이 허용되는지 여부를 확인하는 단계; 및 (d) 실행이 허용되지 않는 명령이면 해당 동작을 수행하지 않고 에러 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 방법에 의해서도 달성된다.

<16> 상기 (a)단계는 상기 명령을 내린 컨텍스트가 로드된 메모리의 플래그를 검사하여 판별하는 단계임이 바람직하다.

<17> 상기 (d)단계는 상기 명령이 AV 데이터의 심리스 재생을 보장하기 위한 마크업 문서의 프리로드 명령이면 프리로드를 수행하지 않고 에러 메시지를 출력하는 단계이거나, 상기 명령이 상기 장치에 마련된 메모리에 프리로드된 데이터에 대한 삭제 명령이면 삭제를 수행하지 않고 에러 메시지를 출력하는 단계이거나, 상기 명령이 상기 장치에 장착된 디스크에 기록된 데이터에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 단계이거나, 상기 명령이 일 프레임을 통한 다른 프레임에의 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 단계이거나, 상기 명령이 타 컨텍스트에 의해 상기 장치에 저장된 쿠키(Cookie)에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 단계이거나, 상기 명령이 상기 장치에서 실행되는 타 컨텍스트에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 단계이거나, 상기 명령이 상기 장치에 장착된 디스크에 기록된 AV 데이터를 재생하는 재생 엔진을 제어하는 명령이면 제어를 수행하지 않고 에러 메시지를 출력하는 단계임이 바람직하다.

<18> 또한, 상기 목적은 네트워크에 접근가능한 장치에 적용가능한 보안 방법에 있어서, (a) 신뢰 컨텍스트가 소정 컨텐트를 읽어올 것을 명령하는 단계; (b) 상기 명령의 신택스를 기초로 신뢰 요구인지 비신뢰 요구인지 여부를 판별하는 단계; 및 (c) 상기 명령이 신뢰 요구이면 상기 컨텐트를 읽어들여 대응하는 신뢰 컨텍스트를 생성하고, 비신뢰 요구이면 대응하는 비신뢰 컨텍스트를 생성하는 단계를 포함하는 것을 특징으로 하는 방법에 의해서도 달성된다.

<19> 상기 (a)단계의 신뢰 컨텍스트는 대응하는 컨텐츠가 상기 장치에 구비된 디스크에 기록되어 있음이 바람직하다.

<20> 상기 (b)단계는 상기 신뢰 컨텍스트의 대응 컨텐트의 내부에 "http:" 요구로 기록되어 있으면 신뢰 요구로 판단하고, "httpu:" 요구로 기록되어 있으면 비신뢰 요구로 판단하는 단계임이 바람직하다.

<21> 한편, 본 발명의 다른 분야에 따르면, 상기 목적은 네트워크에 접속가능한 장치에 의해 재생가능한 정보저장매체에 있어서, 적어도 하나의 어플리케이션 컨텐트를 포함하고, 상기 어플리케이션 컨텐트의 내부에는 신뢰 요구 또는 비신뢰 요구로 해석가능한 명령 정보가 기록되어 있는 것을 특징으로 하는 정보저장매체에 의해서도 달성된다.

<22> 상기 명령 정보는 신뢰 요구 또는 비신뢰 요구를 판별할 수 있는 신택스로 기록됨이 바람직하다.

<23> 상기 신뢰 요구는 "http:" 요구로 기록되고, 상기 비신뢰 요구는 "httpu:" 요구로 기록됨이 더욱 바람직하다.

<24> 한편, 본 발명의 다른 분야에 따르면, 상기 목적은 네트워크에 접근가능한 장치에 있어서, 상기 장치에 장착된 디스크로부터 소정 컨텐트를 읽어들이는 리더; 및 상기 네트워크로부터 소정 컨텐트를 읽어들이는 프리젠테이션 엔진을 포함하고, 상기 프리젠테이션 엔진은 상기 리더를 통해 상기 디스크로부터 읽어들인 컨텐트에 대응하는 제1 신뢰 컨텍스트를 생성하고, 상기 신뢰 컨텍스트로부터 신뢰 요구된 컨텐트는 해석하고 실행하여 제2 신뢰 컨텍스트로 생성하고 상기 제1 신뢰 컨텍스트로부터 비신뢰 요구된 컨텐

트는 해석하고 실행하여 비신뢰 컨텍스트로 생성하는 것을 특징으로 하는 장치에 의해서도 달성된다.

<25> 상기 프리젠테이션 엔진은 소정 컨텐트를 읽어오라는 명령을 내린 컨텍스트가 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 판별하여, 비신뢰 컨텍스트이면 상기 네트워크로부터 상기 컨텐트를 가져와서 대응하는 비신뢰 컨텍스트를 생성하고, 신뢰 컨텍스트이면 상기 명령이 신뢰 요구인지 비신뢰 요구인지 여부를 판별하여 신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 신뢰 컨텍스트를 생성하고, 비신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 것이 바람직하다.

<26> 상기 프리젠테이션 엔진은 상기 명령을 내린 컨텍스트가 로드된 메모리에 함께 기록된 플래그를 검사하여 신뢰 컨텍스트인지 비신뢰 컨텍스트인지를 판별하는 것이 바람직하다.

<27> 상기 프리젠테이션 엔진은 대응하는 컨텐트의 내부에 기록된 신택스를 검사하여 상기 신뢰 컨텍스트로부터의 명령이 신뢰 요구인지 비신뢰 요구인지를 판별하는 것이 효과적이다.

<28> 또한, 상기 목적은 네트워크에 접근가능한 장치에 있어서, 상기 장치에 장착된 디스크로부터 소정 컨텐트를 읽어들이는 리더; 및 상기 네트워크로부터 소정 컨텐트를 읽어들이는 프리젠테이션 엔진을 포함하고, 상기 프리젠테이션 엔진은 상기 리더를 통해 상기 디스크로부터 읽어들인 컨텐트에 대응하는 제1 신뢰 컨텍스트를

생성하고, 상기 제1 신뢰 컨텍스트로부터 신뢰 요구된 컨텐트는 해석하고 실행하여 제2 신뢰 컨텍스트로 생성하고 상기 제1 신뢰 컨텍스트로부터 비신뢰 요구된 컨텐트는 해석하고 실행하여 비신뢰 컨텍스트로 생성하며, 상기 비신뢰 컨텍스트가 내린 소정 동작을 수행하라는 명령이 실행이 허용되지 않는 명령이면 해당 동작을 수행하지 않고 에러 메시지를 출력하는 것을 특징으로 하는 장치에 의해서도 달성된다.

<29> 상기 프리젠테이션 엔진은 상기 비신뢰 컨텍스트로부터 수신된 명령이 AV 데이터의 심리스 재생을 보장하기 위한 마크업 문서의 프리로드 명령이면 프리로드를 수행하지 않고 에러 메시지를 출력하거나, 상기 비신뢰 컨텍스트로부터 수신된 명령이 상기 장치에 구비된 메모리에 프리로드된 데이터에 대한 삭제 명령이면 삭제를 수행하지 않고 에러 메시지를 출력하거나, 상기 비신뢰 컨텍스트로부터 수신된 명령이 상기 장치에 구비된 디스크에 기록된 데이터에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하거나, 상기 비신뢰 컨텍스트로부터 수신된 명령이 일 프레임를 통한 다른 프레임에의 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하거나, 상기 비신뢰 컨텍스트로부터 수신된 명령이 타 컨텍스트에 의해 상기 장치에 저장된 쿠키에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하거나, 상기 비신뢰 컨텍스트로부터 수신된 명령이 상기 장치에서 실행되는 타 컨텍스트에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하거나, 상기 비신뢰 컨텍스트로부터 수신된 명령이 상기 장치에 구비된 디스크에 기록된 AV 데이터를 재생하는 재생 엔진을 제어하는 명령이면 제어를 수행하지 않고 에러 메시지를 출력하는 것이 바람직하다.

<30> 또한, 상기 목적은 네트워크에 접근가능한 장치에 있어서, 상기 장치에 장착된 디스크로부터 소정 컨텐트를 읽어들이는 리더; 및 상기 네트워크로부터 소정 컨텐트를 읽

어들이는 프리젠테이션 엔진을 포함하고, 상기 프리젠테이션 엔진은 상기 리더를 통해 읽어들인 컨텐트로부터 생성된 신뢰 컨텍스트로부터 수신된 소정 컨텐트를 가져오라는 명령의 신택스를 기초로 신뢰 요구인지 비신뢰 요구인지 여부를 판별하여 신뢰 요구이면 요구된 컨텐트를 가져온 다음 그에 대응하는 신뢰 컨텍스트를 생성하고, 비신뢰 요구이면 상기 컨텐트를 가져온 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 것을 특징으로 하는 장치에 의해서도 달성된다.

<31> 상기 프리젠테이션 엔진은 상기 명령이 "http:" 요구이면 신뢰 요구로 판단하고, "httpu:" 요구이면 비신뢰 요구로 판단한다.

<32> 이하 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대해 상세히 설명한다.

<33> 도 1은 본 발명에 따른 보안 방법이 구현되는 보안 시스템의 개요도이다.

<34> 도 1을 참조하면, 보안 시스템은 네트워크의 일 예로서 인터넷에 접속가능하도록 연결된, 본 발명에 따른 재생 장치(1)를 포함한다. 재생 장치(1)는 정보저장매체의 하나인 디스크(10)에 기록된 컨텐트를 읽어들여 실행한다. 나아가, 재생 장치(1)는 인터넷을 통해 적어도 하나의 서버(2,3)에 접속하여 서버(2,3)에 저장된 소정 컨텐트를 가져올 수 있다.

<35> 디스크(10)에는 해석되고 실행되어 프리젠테이션됨으로써 컨텍스트로 생성되는 적어도 하나의 컨텐트가 기록되어 있다. 본 명세서에서 컨텍스트를 생성하는 컨텐트는 특히 어플리케이션 컨텐트라고 부른다. 컨텍스트는 어플리케이션 컨텐트의 인스턴스

(instance)이다. 어플리케이션 컨텐트의 예로는 자바 프로그램, 스크립트 프로그램, 마크업 문서 등을 들 수 있다.

<36> 재생 장치(1)는 컨텐트의 소스(source)를 기준으로 신뢰 컨텐트인지 비신뢰 컨텐트인지 여부를 결정할 수 있다. 본 실시예에서 재생 장치(1)는 디스크(10)로부터 읽어오는 컨텐트는 모두 신뢰 컨텐트로 간주한다. 네트워크에 존재하는 컨텐트는 디스크(10)로부터의 컨텐트로부터 생성된 컨텍스트가 그 컨텐트를 요구하는 명령의 신택스을 해석하여 신뢰 또는 비신뢰로 판단한다.

<37> 컨텐트 제작자는 디스크(10)에 기록되는 어플리케이션 컨텐트를 제작할 때 컨텐트 내부에 신뢰 요구 또는 비신뢰 요구로 해석가능한 신택스로 명령 정보를 기록해둔다. 예를 들어, 마크업 문서와 같은 컨텐트를 제작할 때 링크 태그 등을 이용하여 미리 접속 가능한 서버들, 그 서버들에 대한 신뢰 여부를 결정한 다음, 비신뢰 서버로부터 소정 컨텐트를 가져올 것을 명령하는 명령 정보를 기록할 때는 비신뢰 요구로 해석되는 신택스로 기록하고, 신뢰 서버로부터 소정 컨텐트를 가져올 것을 명령하는 명령 정보를 기록할 때는 신뢰 요구로 해석되는 신택스로 기록한다.

<38> 신뢰 요구와 비신뢰 요구를 구분하는 신택스는 다양하게 결정될 수 있다. 디스크(10)에 기록된 어플리케이션 컨텐트가 마크업 문서의 경우, 네트워크에 존재하는 소정 컨텐트에 대한 신뢰 요구는 "http:" 요구로 기록되고, 비신뢰 요구는 "httpu://" 요구로 기록된다.

<39> 다음은 마크업 문서에 기록된 신뢰 요구인 "http://" 요구의 일 예이다. 재생 장치(1)는 다음과 같은 "http://"요구가 파싱되면 신뢰 요구임을 인식할 수 있다.

<40> ==========

<41> trust

<42> ==========

<43> 마크업 문서에 기록된 비신뢰 "httpu://" 요구의 일 예이다. 마찬가지로, 재생 장치(1)는 다음과 같은 "httpu://"요구가 파싱되면 비신뢰 요구임을 인식할 수 있다.

<44> ==========

<45> untrust

<46> ==========

<47> 신뢰 컨텍스트가 비신뢰 요구로 어떤 컨텐트를 요청하면 재생 장치(1)는 대응 컨텐트를 가져온 다음 그 컨텐트를 실행시켜 비신뢰 컨텍스트로 생성한다. 신뢰 컨텍스트가 신뢰 요구로 어떤 컨텐트를 요청하면 재생 장치(1)는 대응 컨텐트를 가져온 다음 그 컨텐트를 실행시켜 신뢰 컨텍스트로 생성한다.

<48> 재생 장치(1)는 신뢰 컨텍스트가 내리는 명령은 모두 실행시킨다. 그러나, 비신뢰 컨텍스트가 내리는 명령은 제한된 범위 내에서만 실행시킨다. 여기에, 신뢰 컨텍스트와 비신뢰 컨텍스트의 구분 실익이 존재한다. 즉, 비신뢰 컨텍스트의 명령을 미리 결정된 제한된 범위 내에서만 실행시킴으로써 재생 장치(1)의 보안을 유지할 수 있게 된다.

<49> 본 실시예에서 비신뢰 컨텍스트는 신뢰 콘텍스트를 생성할 수 없다. 비신뢰 컨텍스트는 동작 실행에 있어서도 다음과 같은 제한 조건을 가진다.

<50> 1) 비신뢰 컨텍스트는 <프리로드>나 <삭제>와 같은 캐시 제어 접근이 불가하다. <프리로드>와 <삭제>에 대한 상세한 설명은 후술한다.

<51> 2) 비신뢰 컨텍스트가 복수개의 프레임 구조를 갖는 프레임 중의 하나라면 타 프레임에 접근할 수 없다.

<52> 3) 비신뢰 컨텍스트는 다른 컨텍스트가 재생 장치(1)에 저장해둔 쿠키에 접근할 수 없다.

<53> 4) 비신뢰 컨텍스트는 다른 컨텍스트와 데이터를 교환할 수 없다.

<54> 도 2는 재생 장치(1)가 생성한 컨텍스트가 로드된 메모리의 구조도이다.

<55> 도 2를 참조하면, 재생 장치(1)에 구비된 메모리(11)에는 재생 장치(1)가 디스크(10)로부터 읽어들이거나 네트워크로부터 가져온 어플리케이션 컨텐트로부터 생성된 컨텍스트가 로드된다. 이때, 재생 장치(1)는 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 확인할 수 있는 플래그 정보를 함께 기록해둔다. 즉, 메모리(11)에 로드된 컨텍스트는 플래그와 컨텍스트 데이터로 구성된다. 플래그는 대응하는 컨텍스트 데이터가 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 알려준다.

<56> 도 3은 도 1의 재생 장치(1)의 일 실시예이다.

<57> 도 3을 참조하면, 재생 장치(1)는 디스크(100)에 기록된 컨텐트를 재생하는 플레이어로서, 리더(11) 및 프리젠테이션 엔진(12)을 구비한다. 디스크(100)에 기록된 컨텐트는 적어도 하나의 어플리케이션 컨텐트를 포함한다.

<58> 리더(11)는 디스크(100)로부터 어플리케이션 컨텐트를 독출하여 프리젠테이션 엔진(12)으로 제공한다. 프리젠테이션 엔진(12)은 리더(11)를 통해 또는 네트워크로부터 직접 어플리케이션 컨텐트를 가져와서 해석하고 실행하여 컨텍스트를 생성한다.

<59> 본 실시예에서 디스크(100)에는 마크업 문서가 기록되어 있다. <마크업 문서>는 HTML, XML 등의 마크업 언어로 작성된 문서는 물론 스크립트 언어, Java 등으로 작성된 소스 코드가 링크되거나 삽입된 문서를 총칭하며, 나아가 마크업언어 문서에 링크된 파일을 망라하는 마크업 리소스(resource)의 의미로 사용된다. 자바 프로그램이란 Java로 코딩된 프로그램으로써 하나의 장치 또는 네트워크 상에 적어도 일부가 분산되어 존재하는 분산 클라이언트/서버 환경에서 실행되는 응용 프로그램을 말한다. 나아가, 자바 프로그램은 마크업 문서가 해석되어 프리젠테이션되는 마크업 화면의 일부를 구성하며 사용자와 상호작용을 가능하게 해주는 애플릿을 포함한다.

<60> 본 실시예에서 프리젠테이션 엔진(12)은 디스크(100) 또는 네트워크로부터 가져온 마크업 문서 및/또는 자바 프로그램을 해석하여 프리젠테이션함으로써 사용자에게 마크업 화면 및/또는 자바 애플릿을 보여준다.

<61> 도 4는 도 3의 디스크(100)에 컨텐트의 예로서 기록된 마크업 문서 및 자바 프로그램이 해석되고 실행됨으로써 생성되는 컨텍스트를 설명하기 위한 참고도이다.

<62> 도 4를 참조하면, 디스크(100)에는 컨텐트인 마크업 문서 A.HTM, B.HTM, C.HTM, D.HTM와 자바 프로그램 D.JAR가 기록되어 있다. 특히, D.JAR는 JAR 파일로서 자바 애플릿을 위한 클래스, 이미지 및 사운드 파일들을 하나의 파일에 압축하여 담고 있다. JAR 파일은 D.HTM 내에 다음과 같이 정의된다.

<63> ==========

<64> <applet code=AppletClassName archive=JarFileName width=width height=height />

<65> ==========

<66> AppletClassName은 자바 애플릿의 시작 클래스의 이름이고, JarFileName은 자바 애플릿의 클래스들과 관련 이미지 및 사운드 파일이 압축된 JAR 파일의 이름이며, width는 자바 애플릿이 실행되는 화면의 폭이고, height는 자바 애플릿이 실행되는 화면의 높이를 의미한다.

<67> A.HTM는 해석되어 프리젠테이션되어 메인 프레임을 구현하고, B.HTM, C.HTM 및 D.HTM은 각각 해석되고 프리젠테이션되어 각각 서브 프레임을 구현하며, D.JAR는 해석되고 프리젠테이션되어, D.HTM에 의한 서브 프레임 내에서의 자바 애플릿을 구현한다. 이 경우, 컨텍스트는 프레임 단위로 생성된다. 자바 애플릿 또한 하나의 컨텍스트이다. 이처럼 컨텐트는 해석되고 실행되어 프리젠테이션됨으로써 컨텍스트로 생성된다.

<68> 도 5는 도 1의 재생 장치(1)의 다른 실시예이다.

<69> 도 5를 참조하면, 재생 장치(1)는 리더(31), 프리젠테이션 엔진(32), AV 재생 엔진(33) 및 블렌더(34)를 포함한다. 본 실시예의 디스크(300)에 기록된 컨텐트는 마크업 문서 및 자바 프로그램과 더불어 AV 데이터를 포함한다. AV 데이터는 DVD-Video 데이터 포맷으로 기록될 수 있다. 여기서, 어플리케이션 컨텐트는 마크업 문서 및 자바 프로그램을 가리킨다.

<70> 리더(31)는 디스크(300)에 기록된 AV 데이터는 AV 재생 엔진(33)으로 제공하고 디스크(300)에 기록된 마크업 문서 및 자바 프로그램은 프리젠테이션 엔진(32)으로 전달한다.

<71> 프리젠테이션 엔진(32)은 리더(31)를 통해 또는 네트워크로부터 직접 컨텐트를 가져온다. 특히, 어플리케이션 컨텐트는 해석하고 실행하여 컨텍스트를 생성한다. 본 실

시예에서 프리젠테이션 엔진(32)은 디스크(300) 또는 네트워크로부터 가져온 마크업 문서(및/또는 자바 프로그램)을 해석하여 대응 컨텍스트를 생성한다. 즉, 마크업 화면(및/또는 자바 애플릿)을 화면에 띄워준다. 나아가, 프리젠테이션 엔진(32)은 네트워크로부터 AV 데이터를 가져와서 AV 재생 엔진(33)으로 전달해주기도 한다. AV 재생 엔진(33)은 AV 데이터를 재생하여 AV 화면을 출력한다.

<72> 블렌더(34)는 AV 화면 및 마크업 화면을 블렌딩하여 출력한다. 이에, 재생 장치(1)에 마련된 디스플레이 스크린에는 AV 화면이 매립(embedded)된 마크업 화면이 표시된다.

<73> AV 화면이 마크업 화면에 매립되어 디스플레이되는 방식은 종래 알려져 있다. 일예로, PC Friendly사에서는 PC를 기반으로 하여 DVD-Video 데이터를 HTML 문서를 사용하여 재생하는 방식, 즉 DVD-Video 데이터를 재생하여 얻어진 AV 화면을 HTML 문서를 해석하고 실행하여 얻어진 마크업 화면에 매립하여 재생하는 인터렉티브 DVD를 판매하고 있다. 나아가, 본 출원인은 AV 화면을 마크업 화면과 함께 재생하는 다양한 방식 또는 그에 관련된 내용을 담은 선출원을 다수 출원한 바 있다. 예로는 2001년 6월 14일자, 2001년 10월 20일자, 2001년 10월 23일자, 2002년 8월 26일자로 각각 출원된 한국출원 제01-33526호, 제01-64943호, 제01-65391호, 제02-50524호를 들 수 있다.

<74> 도 6은 도 5의 디스크(300)에 컨텐트의 일 예로서 기록된 AV 데이터가 재생되고, 마크업 문서가 해석되고 실행됨으로써 각각 생성되는 컨텍스트를 설명하기 위한 참고도이다.

<75> 도 6을 참조하면, 디스크(300)에는 컨텐트인 AV 데이터와 마크업 문서 E.HTM이 기록되어 있다. AV 데이터는 AV 재생 엔진(33)에 의해 재생되어 AV 화면을 구현하고,

E.HTM는 해석되고 프리젠테이션되어 메인 프레임인 마크업 화면을 구현한다. 여기서, 마크업 화면은 컨텍스트이다.

<76> 도 7은 도 5의 디스크(300)에 컨텐트의 다른 예로서 기록된 AV 데이터가 재생되고, 마크업 문서 및 자바 프로그램이 해석되고 실행됨으로써 각각 생성되는 컨텍스트를 설명하기 위한 참고도이다.

<77> 도 7을 참조하면, 디스크(300)에는 컨텐트인 AV 데이터와 마크업 문서 F.HTM, 및 자바 프로그램 F.JAR이 기록되어 있다. AV 데이터는 AV 재생 엔진(33)에 의해 재생되어 AV 화면을 구현하고, F.HTM는 해석되고 프리젠테이션되어 메인 프레임인 마크업 화면을 구현한다. F.JAR는 F.HTM 내에 정의되어, 마크업 화면에서 실행되는 자바 애플릿을 구현한다. 여기서, 마크업 화면 및 자바 애플릿은 컨텍스트이다. 이처럼 어플리케이션 컨텐트는 해석되고 실행되어 프리젠테이션됨으로써 컨텍스트로 생성된다.

<78> 상기와 같은 구성을 기초로 본 발명의 바람직한 실시예에 따른 보안 방법을 설명하면 다음과 같다.

<79> 도 8은 본 발명의 일 실시예에 따른 보안 방법을 설명하기 위한 플로우챠트이다.

<80> 도 8을 참조하면, 재생 장치(1)는 일 컨텍스트가 타 컨텐트를 디스크 또는 네트워크로부터 읽어올 것을 명령하면(801단계), 그 명령을 내린 컨텍스트가 신뢰 컨텍스트의 명령인지 여부를 판별한다(802단계). 신뢰 컨텍스트인지 여부는 재생 장치(1)가 대응 컨텐트를 읽어올 때 함께 메모리(11)에 저장해둔 플래그를 보면 알 수 있다. 비신뢰 컨텍스트이면 재생 장치(1)는 명령받은 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨

텍스트를 생성한다(803단계). 신뢰 컨텍스트이면 대응하는 컨텍스트의 요구가 신뢰 요구인지 비신뢰 요구인지 여부를 판별한다(804단계). 신뢰 요구인지 비신뢰 요구인지 판별은 예를 들면, 마크업 문서(컨텐트)에 기록된 명령 정보의 신택스를 보면 알 수 있다. 마크업 문서에는 신뢰 요구는 "http://" 요구로 기록되고, 비신뢰 요구는 "httpu://" 요구로 기록된다. 신뢰 요구이면 재생 장치(1)는 명령받은 컨텐트를 읽어들인 다음 그에 대응하는 신뢰 컨텍스트를 생성한다(805단계). 비신뢰 요구이면 명령받은 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨텍스트를 생성한다(806단계).

<81> 도 9는 본 발명의 다른 실시예에 따른 보안 방법을 설명하기 위한 플로우챠트이다.

<82> 도 9를 참조하면, 재생 장치(1)는 일 컨텍스트가 소정 동작을 수행하라는 명령을 내리면(901단계), 명령을 내린 컨텍스트가 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 확인한다(902단계). 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부는 마찬가지로 메모리(11)에 기록해둔 플래그를 보면 알 수 있다. 신뢰 컨텍스트의 명령이면 재생 장치(1)는 명령을 실행한다(903단계). 비신뢰 컨텍스트의 명령이면 재생 장치(1)는 실행이 허용되지 않는 명령인지 아닌지 여부를 확인한다(904단계). 비신뢰 컨텍스트의 실행 범위는 전술한 바와 같이 미리 결정된다. 즉, 재생 장치(1)는 비신뢰 컨텍스트의 동작의 허용 범위를 미리 알고 있다. 실행이 허용되면 재생 장치(1)는 해당 동작을 실행한다(905단계). 실행이 허용되지 않으면 재생 장치(1)는 해당 동작을 수행하지 않고 에러 메시지를 출력한다(906단계).

<83> 906단계의 구체적인 예들은 다음과 같다.

<84> 예 1. 비신뢰 컨텍스트의 명령이 AV 데이터의 심리스 재생을 보장하기 위한 마크업 문서의 프리로드 명령이면 도 5의 재생 장치(1)는 프리로드를 수행하지 않고 에러 메시

지를 출력한다. <프리로드>는 심리스 재생이 보장되는 AV 데이터를 마크업 문서와 함께 재생할 때 마크업 문서를 읽어들이기 위해 소요되는 시간으로 인해 버퍼링되는 AV 데이터가 소진되어 AV 데이터의 재생이 끊기는 현상이 나타나지 않도록 하기 위해 미리 마크업 문서들을 도 5의 재생 장치(1)에 마련된 메모리(도시되지 않음)에 로딩해두는 것을 의미한다. 비신뢰 컨텍스트의 명령이 재생 장치(1)에 마련된 메모리(도시되지 않음)에 프리로드된 데이터에 대한 삭제 명령이면 삭제를 수행하지 않고 에러 메시지를 출력한다. <프리로드> 및 프리로드된 데이터의 <삭제>에 대한 보다 상세한 설명은 본 출원인이 2002년 9월 19일자로 출원한 한국출원 제02-57393호 <프리로드 정보가 기록된 정보저장 매체, 그 재생장치 및 재생방법>에 기재되어 있다.

<85> 예 2. 비신뢰 컨텍스트의 명령이 재생 장치(1)에 장착된 디스크에 기록된 데이터에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력한다.

<86> 예 3. 비신뢰 컨텍스트가 도 4에 도시된 바와 같이 복수개의 프레임들 중 어느 하나인 경우, 비신뢰 컨텍스트의 명령이 자신의 프레임이 아닌 타 프레임에의 접근 명령이면 재생 장치(1)는 접근을 수행하지 않고 에러 메시지를 출력한다.

<87> 예 4. 비신뢰 컨텍스트의 명령이 타 컨텍스트에 의해 재생 장치(1)에 저장된 쿠키에 대한 접근 명령이면 재생 장치(1)는 접근을 수행하지 않고 에러 메시지를 출력한다.

<88> 예 5. 비신뢰 컨텍스트의 명령이 재생 장치(1)에서 실행되는 타 컨텍스트에 대한 접근 명령이면 재생 장치(1)는 접근을 수행하지 않고 에러 메시지를 출력한다.

<89> 예 6. 비신뢰 컨텍스트의 명령이 도 5의 재생 장치(1)에 장착된 디스크에 기록된 AV 데이터를 재생하는 AV 재생 엔진(33)을 제어하는 명령이면, 도 5의 재생 장치(1)는 제어를 수행하지 않고 에러 메시지를 출력한다.

【발명의 효과】

<90> 전술한 바와 같이, 본 발명에 따르면 네트워크에 접근가능한 장치에 있어서 네트워크로부터 읽어들인 컨텐트에 대응하는 컨텍스트에 대한 보안을 강화할 수 있는 보안 방법, 그 장치 및 정보저장매체가 제공된다. 이에 의해, 네트워크로부터 읽어들인 컨텐트에 대응하는 비신뢰 컨텍스트가 장치에 저장된 중요한 정보를 파괴시키거나 외부로 유출하는 등의 경우를 미연에 방지할 수 있다.

【특허청구범위】

【청구항 1】

네트워크에 접근가능한 장치에 적용가능한 보안 방법에 있어서,

(a) 소정 컨텐트를 읽어오라는 명령을 내린 컨텍스트가 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 판별하는 단계;

(b) 비신뢰 컨텍스트이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 단계;

(c) 상기 컨텍스트가 신뢰 컨텍스트이면 상기 명령이 신뢰 요구인지 비신뢰 요구인지 여부를 판별하는 단계;

(d) 상기 명령이 신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 신뢰 컨텍스트를 생성하는 단계; 및

(e) 상기 명령이 비신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 2】

제1항에 있어서,

상기 (a)단계는

상기 명령을 내린 컨텍스트가 로드된 메모리의 플래그를 검사하여 판별하는 단계임을 특징으로 하는 방법.

【청구항 3】

네트워크에 접근가능한 장치에 적용가능한 보안 방법에 있어서,

(a) 컨텍스트가 동작 명령을 내리는 단계;

(b) 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 판별하는 단계;

(c) 비신뢰 컨텍스트이면 상기 동작 명령의 실행이 허용되는지 여부를 확인하는 단계; 및

(d) 실행이 허용되지 않는 명령이면 해당 동작을 수행하지 않고 에러 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 4】

제3항에 있어서,

상기 (a)단계는

상기 명령을 내린 컨텍스트가 로드된 메모리의 플래그를 검사하여 판별하는 단계임을 특징으로 하는 방법.

【청구항 5】

제3항에 있어서,

상기 (d)단계는

AV 데이터의 심리스 재생을 보장하기 위한 마크업 문서의 프리로드 명령이면 프리로드를 수행하지 않고 에러 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 6】

제3항에 있어서,

상기 (d)단계는

상기 명령이 상기 장치에 마련된 메모리에 프리로드된 데이터에 대한 삭제 명령이면 삭제를 수행하지 않고 에러 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 7】

제3항에 있어서,

상기 (d)단계는

상기 명령이 상기 장치에 장착된 디스크에 기록된 데이터에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 8】

제3항에 있어서,

상기 (d)단계는

상기 명령이 일 프레임를 통한 다른 프레임에의 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 9】

제3항에 있어서,

상기 (d)단계는

타 컨텍스트에 의해 상기 장치에 저장된 쿠키(Cookie)에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 10】

제3항에 있어서,

상기 (d)단계는

상기 명령이 상기 장치에서 실행되는 타 컨텍스트에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 11】

제3항에 있어서,

상기 (d)단계는

상기 명령이 상기 장치에 장착된 디스크에 기록된 AV 데이터를 재생하는 재생 엔진을 제어하는 명령이면 제어를 수행하지 않고 에러 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 12】

네트워크에 접근가능한 장치에 적용가능한 보안 방법에 있어서,

(a) 신뢰 컨텍스트가 소정 컨텐트를 읽어올 것을 명령하는 단계;

(b) 명령의 신택스를 기초로 신뢰 요구인지 비신뢰 요구인지 여부를 판별하는 단계; 및

(c) 상기 명령이 신뢰 요구이면 상기 컨텐트를 읽어들여 대응하는 신뢰 컨텍스트를 생성하고, 비신뢰 요구이면 대응하는 비신뢰 컨텍스트를 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

【청구항 13】

제12항에 있어서,

상기 (a)단계의 신뢰 컨텍스트는 대응하는 컨텐츠가 상기 장치에 구비된 디스크에 기록되어 있음을 특징으로 하는 방법.

【청구항 14】

제13항에 있어서,

상기 (b)단계는

상기 신뢰 컨텍스트의 대응 컨텐트의 내부에 "http:" 요구로 기록되어 있으면 신뢰 요구로 판단하고, "httpu:" 요구로 기록되어 있으면 비신뢰 요구로 판단하는 단계임을 특징으로 하는 방법.

【청구항 15】

네트워크에 접속가능한 장치에 의해 재생가능한 정보저장매체에 있어서,

적어도 하나의 어플리케이션 컨텐트를 포함하고,

상기 어플리케이션 컨텐트의 내부에는 신뢰 요구 또는 비신뢰 요구로 해석가능한 명령 정보가 기록되어 있는 것을 특징으로 하는 정보저장매체.

【청구항 16】

제15항에 있어서,

상기 명령 정보는 신뢰 요구 또는 비신뢰 요구를 판별할 수 있는 신택스로 기록됨을 특징으로 하는 정보저장매체.

【청구항 17】

제16항에 있어서,

상기 신뢰 요구는 "http:" 요구로 기록되고, 상기 비신뢰 요구는 "httpu:" 요구로 기록됨을 특징으로 하는 정보저장매체.

【청구항 18】

제17항에 있어서,

상기 "http:" 요구는 상기 네트워크에 존재하는 신뢰 컨텐트를 읽어올 것을 요구하는 명령임을 특징으로 하는 정보저장매체.

【청구항 19】

제17항에 있어서,

상기 "httpu:" 요구는 상기 네트워크에 존재하는 비신뢰 컨텐트를 읽어올 것을 요구하는 명령임을 특징으로 하는 정보저장매체.

【청구항 20】

네트워크에 접근가능한 장치에 있어서,

상기 장치에 장착된 디스크로부터 소정 컨텐트를 읽어들이는 리더; 및

상기 네트워크로부터 소정 컨텐트를 읽어들이는 프리젠테이션 엔진을 포함하고,

상기 프리젠테이션 엔진은 상기 리더를 통해 상기 디스크로부터 읽어들인 컨텐트에 대응하는 제1 신뢰 컨텍스트를 생성하고, 상기 신뢰 컨텍스트로부터 신뢰 요구된 컨텐트는 해석하고 실행하여 제2 신뢰 컨텍스트로 생성하고 상기 제1 신뢰 컨텍스트로부터 비신뢰 요구된 컨텐트는 해석하고 실행하여 비신뢰 컨텍스트로 생성하는 것을 특징으로 하는 장치.

【청구항 21】

제20항에 있어서,

상기 프리젠테이션 엔진은

소정 컨텐트를 읽어오라는 명령을 내린 컨텍스트가 신뢰 컨텍스트인지 비신뢰 컨텍스트인지 여부를 판별하여,

비신뢰 컨텍스트이면 상기 네트워크로부터 상기 컨텐트를 가져와서 대응하는 비신뢰 컨텍스트를 생성하고, 신뢰 컨텍스트이면 상기 명령이 신뢰 요구인지 비신뢰 요구인지 여부를 판별하여 신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 신뢰 컨텍스트를 생성하고, 비신뢰 요구이면 상기 컨텐트를 읽어들인 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 것을 특징으로 하는 장치.

【청구항 22】

제20항에 있어서,

상기 프리젠테이션 엔진은 상기 명령을 내린 컨텍스트가 로드된 메모리에 함께 기록된 플래그를 검사하여 신뢰 컨텍스트인지 비신뢰 컨텍스트인지를 판별하는 것을 특징으로 하는 장치.

【청구항 23】

제20항에 있어서,

상기 프리젠테이션 엔진은

대응하는 컨텐트의 내부에 기록된 신택스를 검사하여 상기 신뢰 컨텍스트로부터의 명령이 신뢰 요구인지 비신뢰 요구인지를 판별하는 것을 특징으로 하는 장치.

【청구항 24】

네트워크에 접근가능한 장치에 있어서,

상기 장치에 장착된 디스크로부터 소정 컨텐트를 읽어들이는 리더; 및

상기 네트워크로부터 소정 컨텐트를 읽어들이는 프리젠테이션 엔진을 포함하고,

상기 프리젠테이션 엔진은 상기 리더를 통해 상기 디스크로부터 읽어들인 컨텐트에 대응하는 제1 신뢰 컨텍스트를 생성하고, 상기 제1 신뢰 컨텍스트로부터 신뢰 요구된 컨텐트는 해석하고 실행하여 제2 신뢰 컨텍스트로 생성하고 상기 제1 신뢰 컨텍스트로부터 비신뢰 요구된 컨텐트는 해석하고 실행하여 비신뢰 컨텍스트로 생성하며, 상기 비신뢰 컨텍스트가 내린 소정 동작을 수행하라는 명령이 실행이 허용되지 않는 명령이면 해당 동작을 수행하지 않고 에러 메시지를 출력하는 것을 특징으로 하는 장치.

【청구항 25】

제24항에 있어서,

상기 프리젠테이션 엔진은

상기 비신뢰 컨텍스트로부터 수신된 명령이 AV 데이터의 심리스 재생을 보장하기 위한 마크업 문서의 프리로드 명령이면 프리로드를 수행하지 않고 에러 메시지를 출력하는 것을 특징으로 하는 장치.

【청구항 26】

제24항에 있어서,

상기 프리젠테이션 엔진은

상기 비신뢰 컨텍스트로부터 수신된 명령이 상기 장치에 구비된 메모리에 프리로드된 데이터에 대한 삭제 명령이면 삭제를 수행하지 않고 에러 메시지를 출력하는 것을 특징으로 하는 장치.

【청구항 27】

제24항에 있어서,

상기 프리젠테이션 엔진은

상기 비신뢰 컨텍스트로부터 수신된 명령이 상기 장치에 구비된 디스크에 기록된 데이터에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 것을 특징으로 하는 장치.

【청구항 28】

제24항에 있어서,

상기 프리젠테이션 엔진은

상기 비신뢰 컨텍스트로부터 수신된 명령이 일 프레임를 통한 다른 프레임에의 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 것을 특징으로 하는 장치.

【청구항 29】

제24항에 있어서,

상기 프리젠테이션 엔진은

상기 비신뢰 컨텍스트로부터 수신된 명령이 타 컨텍스트에 의해 상기 장치에 저장된 쿠키(Cookie)에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 것을 특징으로 하는 장치.

【청구항 30】

제24항에 있어서,

상기 프리젠테이션 엔진은

상기 비신뢰 컨텍스트로부터 수신된 명령이 상기 장치에서 실행되는 타 컨텍스트에 대한 접근 명령이면 접근을 수행하지 않고 에러 메시지를 출력하는 것을 특징으로 하는 장치.

【청구항 31】

제24항에 있어서,

상기 프리젠테이션 엔진은

상기 비신뢰 컨텍스트로부터 수신된 명령이 상기 장치에 구비된 디스크에 기록된 AV 데이터를 재생하는 재생 엔진을 제어하는 명령이면 제어를 수행하지 않고 에러 메시지를 출력하는 것을 특징으로 하는 장치.

【청구항 32】

네트워크에 접근가능한 장치에 있어서,

상기 장치에 장착된 디스크로부터 소정 컨텐트를 읽어들이는 리더; 및

상기 네트워크로부터 소정 컨텐트를 읽어들이는 프리젠테이션 엔진을 포함하고,

상기 프리젠테이션 엔진은 상기 리더를 통해 읽어들인 컨텐트로부터 생성된 신뢰 컨텍스트로부터 수신된 소정 컨텐트를 가져오라는 명령의 신택스를 기초로 신뢰 요구인지 비신뢰 요구인지 여부를 판별하여 신뢰 요구이면 요구된 컨텐트를 가져온 다음 그에

대응하는 신뢰 컨텍스트를 생성하고, 비신뢰 요구이면 상기 컨텐트를 가져온 다음 그에 대응하는 비신뢰 컨텍스트를 생성하는 것을 특징으로 하는 장치.

【청구항 33】

제32항에 있어서,

상기 프리젠테이션 엔진은

상기 명령이 "http:" 요구이면 신뢰 요구로 판단하고, "httpu:" 요구이면 비신뢰 요구로 판단하는 것을 특징으로 하는 장치.

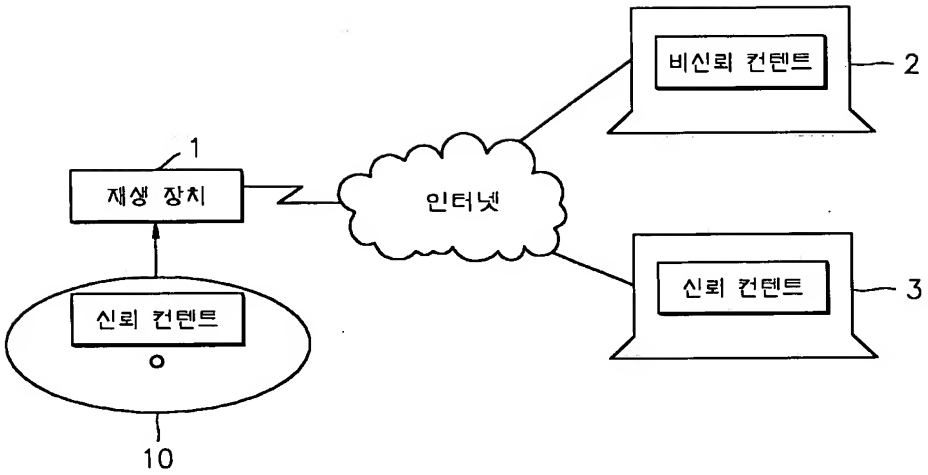
【청구항 34】

제32항에 있어서,

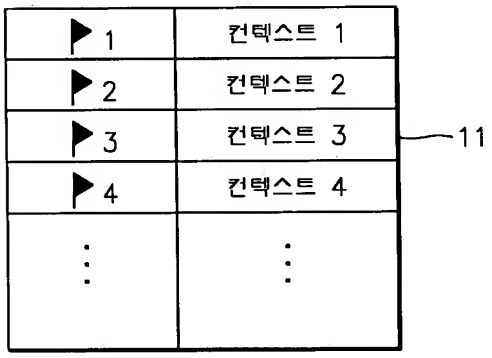
상기 컨텐트는 상기 장치에 의해 해석되고 실행되는 자바 프로그램, 스크립트 프로그램 및 마크업 문서 중 적어도 하나임을 특징으로 하는 장치.

【도면】

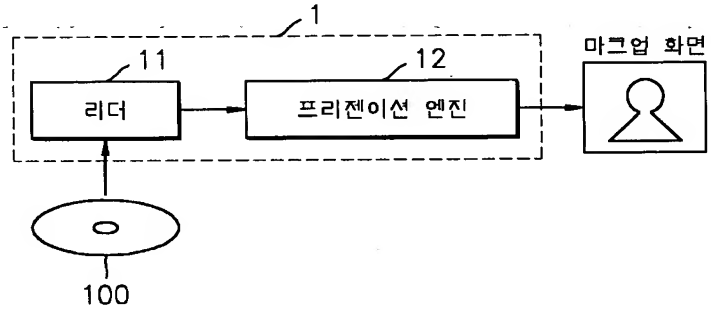
【도 1】


비신뢰 컨텐트
2
1
재생 장치
인터넷
신뢰 컨텐트
3
신뢰 컨텐트
10

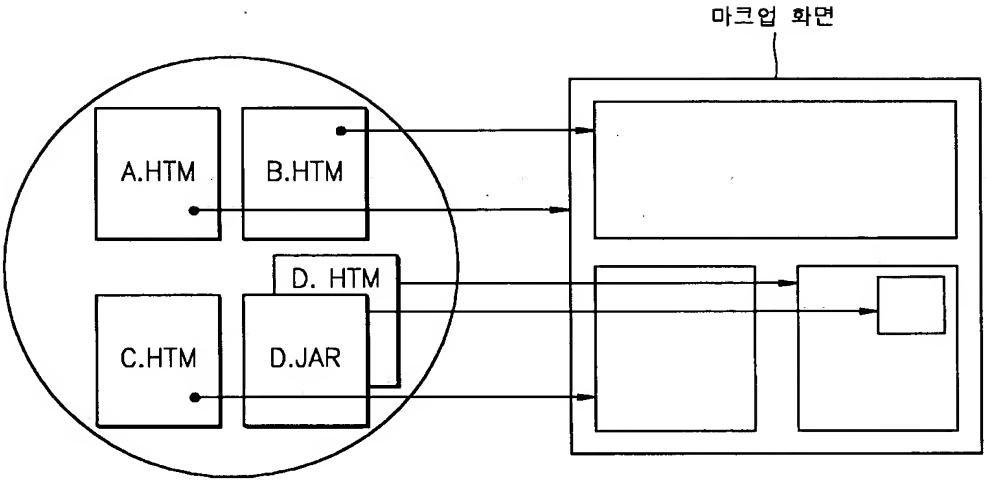
【도 2】


1
컨텍스트 1
2
컨텍스트 2
3
컨텍스트 3
11
4
컨텍스트 4

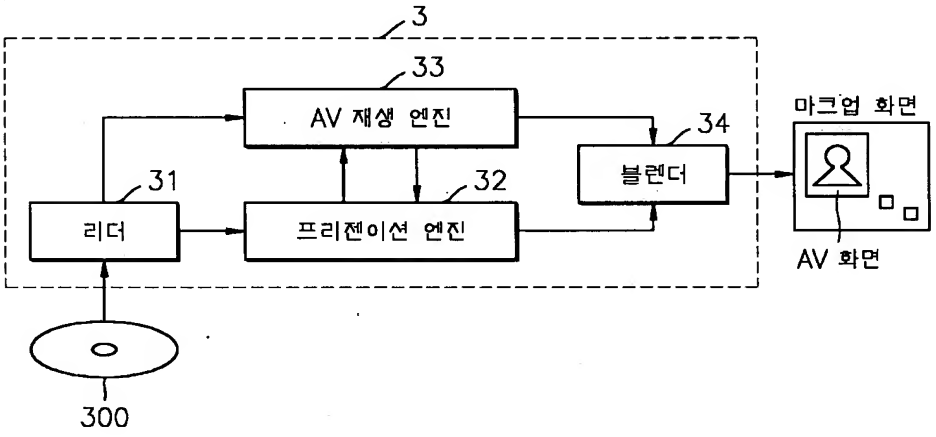
【도 3】


1
11
12
마크업 화면
리더
프리젠이션 엔진
100

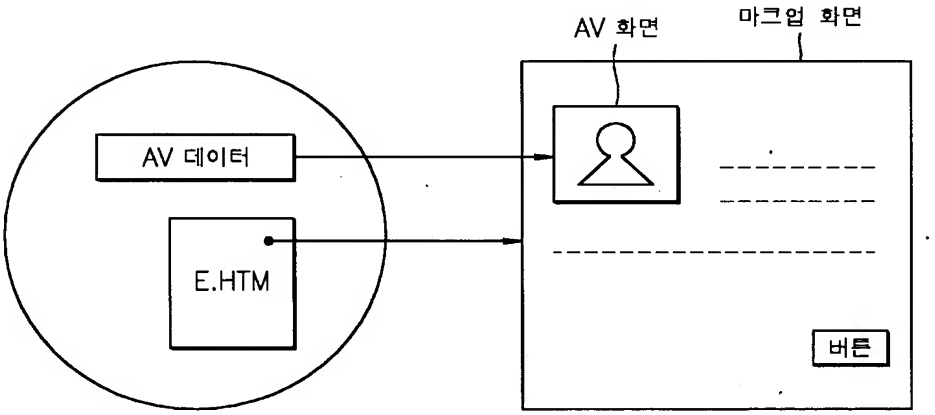
【도 4】


마크업 화면
A.HTM
B.HTM
D. HTM
C.HTM
D.JAR

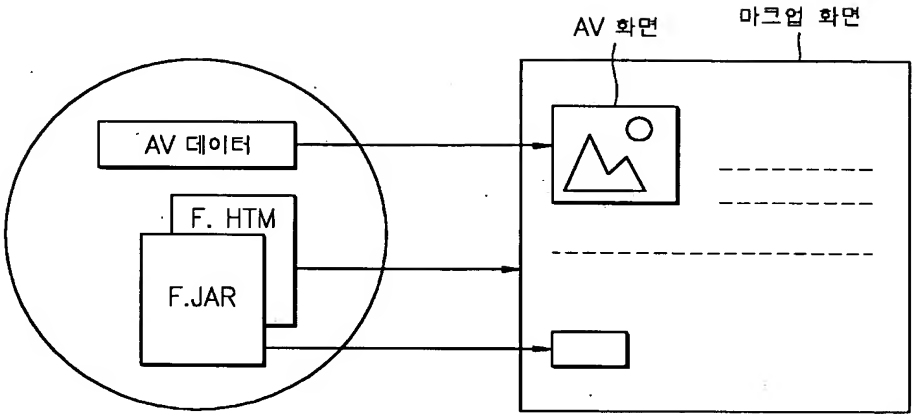
【도 5】


3
33
AV 재생 엔진
34
마크업 화면
31
32
블렌더
리더
프리젠이션 엔진
AV 화면
300

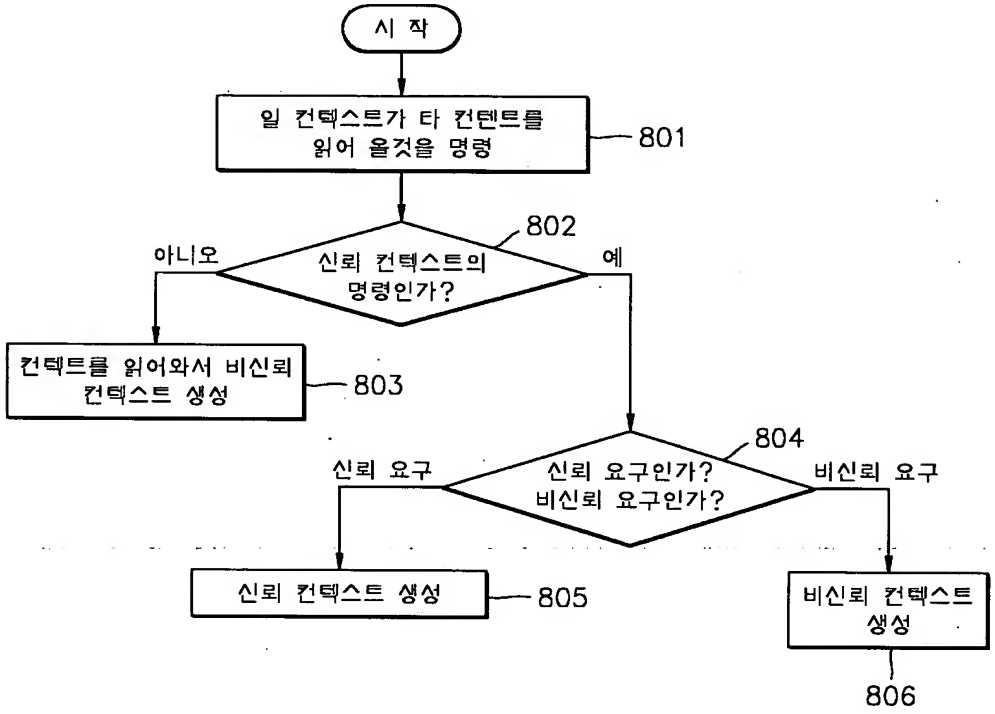
【도 6】


AV 화면
마크업 화면
AV 데이터
E.HTM
버튼

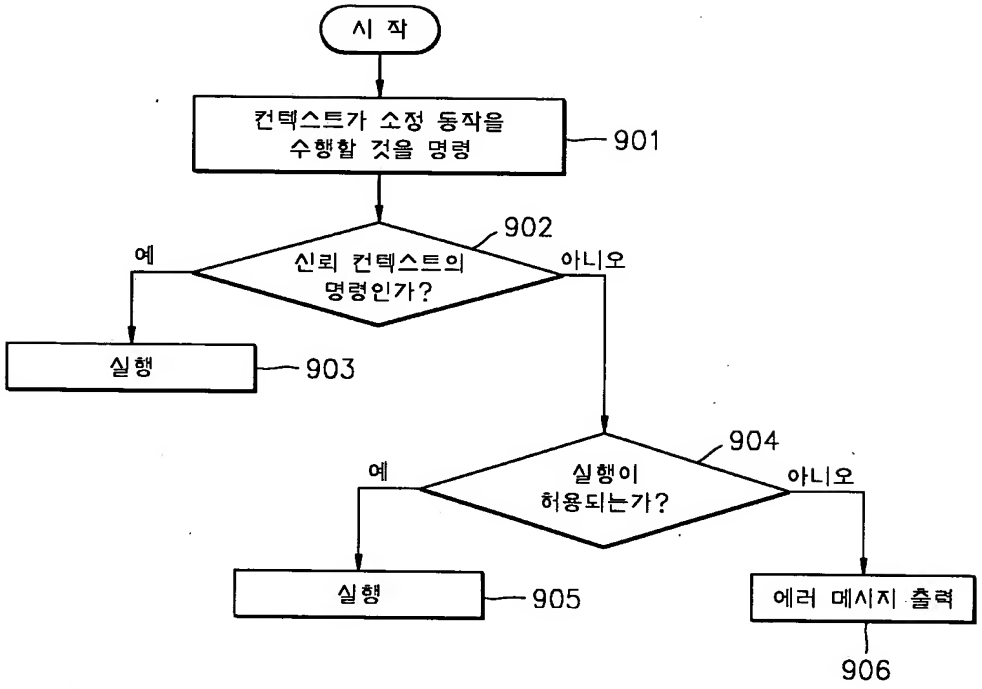
【도 7】


AV 화면
마크업 화면
AV 데이터
F. HTM
F.JAR

【도 8】


시 작
일 컨텍스트가 타 컨텐트를 읽어 올것을 명령
801
802
신뢰 컨텍스트의 명령인가?
아니오
예
컨텍트를 읽어와서 비신뢰 컨텍스트 생성
803
804
신뢰 요구인가? 비신뢰 요구인가?
신뢰 요구
비신뢰 요구
신뢰 컨텍스트 생성
805
비신뢰 컨텍스트 생성
806

【도 9】


시 작
컨텍스트가 소정 동작을 수행할 것을 명령
901
902
신뢰 컨텍스트의 명령인가?
예
아니오
실행
903
904
실행이 허용되는가?
예
아니오
실행
905
에러 메시지 출력
906